vSphere Host Profiles

Update 3
VMware vSphere 8.0
VMware ESXi 8.0
vCenter Server 8.0



You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About vSphere® Host Profiles

The *vSphere Host Profiles* documentation describes how to manage and configure Host Profiles in the vSphere Client.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

The *vSphere Host Profiles* documentation is intended for administrators who are familiar with vSphere host configuration.

What Are vSphere Host Profiles

1

The vSphere Host Profiles are profiles that encapsulate the host configuration and help to manage the host configuration, especially in environments where an administrator manages multiple hosts or clusters in vCenter Server.

Host Profiles provide an automated and centrally managed mechanism for host configuration and configuration compliance. Host Profiles can improve efficiency by reducing reliance upon repetitive, manual tasks. Host Profiles capture the configuration of a pre-configured and validated reference host, store the configuration as a managed object and use the catalog of parameters contained within to configure networking, storage, security, and other host-level parameters. Host Profiles can be applied to individual hosts, a cluster, or all the hosts and clusters associated to a host profile. Applying a Host Profile to a cluster affects all hosts in the cluster and results in a consistent configuration across the applied hosts.

Host Profiles can be used to validate the configuration of a host by checking compliance of a host or cluster against the Host Profile that is associated with that host or cluster.

Read the following topics next:

- Reference Host Independence
- Reference Host Selection
- Host Profiles and vSphere Auto Deploy

Reference Host Independence

A dedicated reference host is not required to be available to perform host profile tasks.

When you create a host profile, you extract the configuration information from a specified ESXi reference host. In previous releases, vSphere required that the reference host was available for certain Host Profiles tasks, such as editing, importing, and exporting. From vSphere 6.0 and later, a dedicated reference host is no longer required to be available to perform these tasks. For host profile tasks that require a reference host, an ESXi host that is compatible to the host profile is assigned as a reference host.

Sometimes, a compatible host is not available to validate the host profile during these tasks. If you make small changes to the host profile, validation is skipped and a you see a warning indicating that no valid reference host is associated with the profile. You can then proceed and finish the task.

Due to the introduction of this feature, users can no longer edit or change the reference host from the vSphere Client. The reference host selection occurs at runtime, without notifying users, in the vCenter Server for on-going tasks.

Reference Host Selection

To select a suitable reference host, vCenter Server performs complex version and compatibility checks on the target host.

Starting with vSphere 7.0 Update 3, a major-version vCenter Server instance can manage hosts of all ESXi Update release versions within the respective major version. For example, a vCenter Server 7.0 Update 3 instance can manage ESXi hosts and hosts profiles of version 7.0 GA, 7.0 Update 1, 7.0 Update 2, and 7.0 Update 3. This change affects the reference host selection for particular host profile operations.

Version Check

To select a reference host, vCenter Server checks whether the target host is of the same ESXi Update release version as the host profile. For some operations, the target host can run a later ESXi version than the ESXi version of the host profile. For example, if you want to edit a 7.0 Update 3 host profile, the reference host that validates the host profile cannot be running ESXi 7.0 GA, 7.0 Update 1, or 7.0 Update 2.

Compatibility Check

In addition to checking the version on the target host, vCenter Server performs an extensive compatibility check that includes a subprofile compatibility check in the existing releases. Starting with vSphere 7.0 Update 3, to appoint a reference host, vCenter Server checks the advanced options and the default roles in the target host. A reference host must support the advanced options of the host profile it validates. Also, the default roles in the reference host must match the default roles in the host profile.

Host Profile Operations and Required Reference Host Versions

A reference host is needed to validate the host profile during different host profile operations and workflows. Starting with vSphere 7.0 Update 3, depending on the operation, the reference host must be of exactly the same or later Update release version as the host profile it validates. The following table summarizes the compatible reference host versions for different host profile operations if your environment runs a vCenter Server instance 7.0 Update 3 or later.

Host Profile Operation	Compatible Reference Host Version
Edit	The same Update release version as the host profile.
Check Compliance	The same or later Update release version as the host profile.
Remediation	The same or later Update release version as the host profile.

Host Profile Operation	Compatible Reference Host Version
Attach	The same or later version as the host profile.
Import/Export	The exact same version as the host profile.

Note If the vCenter Server instance is of version earlier than 7.0 Update 3, Update release versions are not checked during the selection of a reference host. vCenter Server only checks if the reference host and the host profile are of the same major release version, for example 6.x or 7.x.

Host Profiles and vSphere Auto Deploy

You can use Host Profiles and vSphere Auto Deploy to provision physical ESXi hosts with a complete and expected configuration state for virtual switches, driver settings, boot parameters, and so on.

Because hosts that are provisioned with Auto Deploy are considered to be stateless, configuration state information is not stored on the host. Instead, you create and configure a reference host. Then, you create a host profile from the reference host. Next, you associate the host profile with an Auto Deploy rule. As a result new hosts that you provision with Auto Deploy have the host profile applied automatically.

Remediation for these hosts is the same as statefully deployed hosts. When you apply the host profile, you are prompted to customize the hosts and enter answers for the policies that you specified during the host profile creation.

Note If you deploy ESXi with Auto Deploy, configure a `syslog` to store logs in a remote server. For more information on setting up a syslog from the Host Profiles interface, see the *vSphere Installation and Setup* documentation.

For more information on setting up an Auto Deploy reference host, see the *VMware ESXi Installation and Setup* documentation.

How Do You Manage vSphere Host Profiles in the vSphere Client

2

By using the vSphere Client, you can perform basic tasks for host profiles, perform and schedule compliance checks of hosts and clusters, remediate hosts which are not compliant with the attached host profiles.

Host Profiles Usage Model

The Host Profiles workflow starts with the concept of a reference host. The configuration of the reference host, which is extracted as a host profile, serves as a configuration template for configuring other hosts. The reference host does not have to be related or associated with the host profile extracted from it.

Before you begin, ensure that you have an existing vSphere environment installation with at least one properly configured ESXi host.

The sequence required to create a host profile from a reference host, apply the host profile to a host or cluster and check compliance against the host profile is as follows:

1. Set up and configure the reference host.
2. Create a host profile from the reference host.
3. Attach hosts or clusters to the host profile.
4. Check the compliance to the host profile. If all hosts are compliant with the reference host, they are correctly configured.
5. Apply (remediate).

As a licensed feature of vSphere, Host Profiles are only available when the appropriate licensing is in place. If you see errors, ensure that you have the appropriate vSphere licensing for your hosts.

If you want the Host Profile to use directory services for authentication, configure the reference host to use a directory service. See the *vSphere Security* documentation.

Hosts Provisioned with vSphere Auto Deploy

For hosts provisioned with vSphere Auto Deploy, the vSphere Client owns the entire host configuration, which is captured in a Host Profile. Usually, the Host Profile information is sufficient to store all configuration information. Sometimes the user is prompted for input when the host provisioned with Auto Deploy starts. See the *VMware ESXi Installation and Setup* documentation for more information on Auto Deploy.

Read the following topics next:

- How Do You Get Started with vSphere Host Profiles
- How Do You Manage Compliance Checks of Hosts and Clusters to a vSphere Host Profile

How Do You Get Started with vSphere Host Profiles

Learn how to create a host profile, attach or detach hosts and clusters to a host profile, import or export a host profile, duplicate a host profile, and copy settings from a reference host to a host profile or from one host profile to another.

Note When vSphere Configuration Profiles is enabled on a cluster, you cannot attach or edit host profiles in the cluster or in the hosts in that cluster. For more information on vSphere Configuration Profiles, see the *Managing Host and Cluster Lifecycle* guide.

How Do You Create a vSphere Host Profile?

You create a host profile by extracting the configuration from a designated reference host.

Host profiles do not capture offline or non-present devices. Any changes made to offline devices after extracting a host profile do not make a difference to the compliance check results.

Note When vSphere Configuration Profiles is enabled on a cluster, you cannot attach or edit host profiles in the cluster or in the hosts in that cluster. For more information on vSphere Configuration Profiles, see the *Managing Host and Cluster Lifecycle* guide.

Prerequisites

Verify that you have a working vSphere installation and at least one completely and properly configured host.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Click **Extract Host Profile**.

4 On the **Select host** page, select the vCenter Server instance where to create the host profile.

5 Select the host that acts as the reference host and click **Next**.

The selected host must be a valid host.

6 Enter a name and, optionally, a description for the new profile, and click **Finish**.

Results

The new profile appears in the **Host Profiles** pane.

How Do You Attach or Detach Hosts and Clusters to a vSphere Host Profile?

After you create a host profile from a reference host, you must attach a host or a cluster to the host profile to associate that host profile with the selected host or cluster. To disassociate a configuration from an ESXi host or an entire cluster, detach the host or cluster from the host profile.

When a host profile is attached to a cluster, the host or hosts within that cluster are also attached to the host profile. However, when the host profile is detached from the entire cluster, there is no association between the host or hosts within the cluster and that host profile. Detaching a host profile from an ESXi host or a cluster does not delete that host profile. You can delete the host profile after detaching it from all the entities it is associated with.

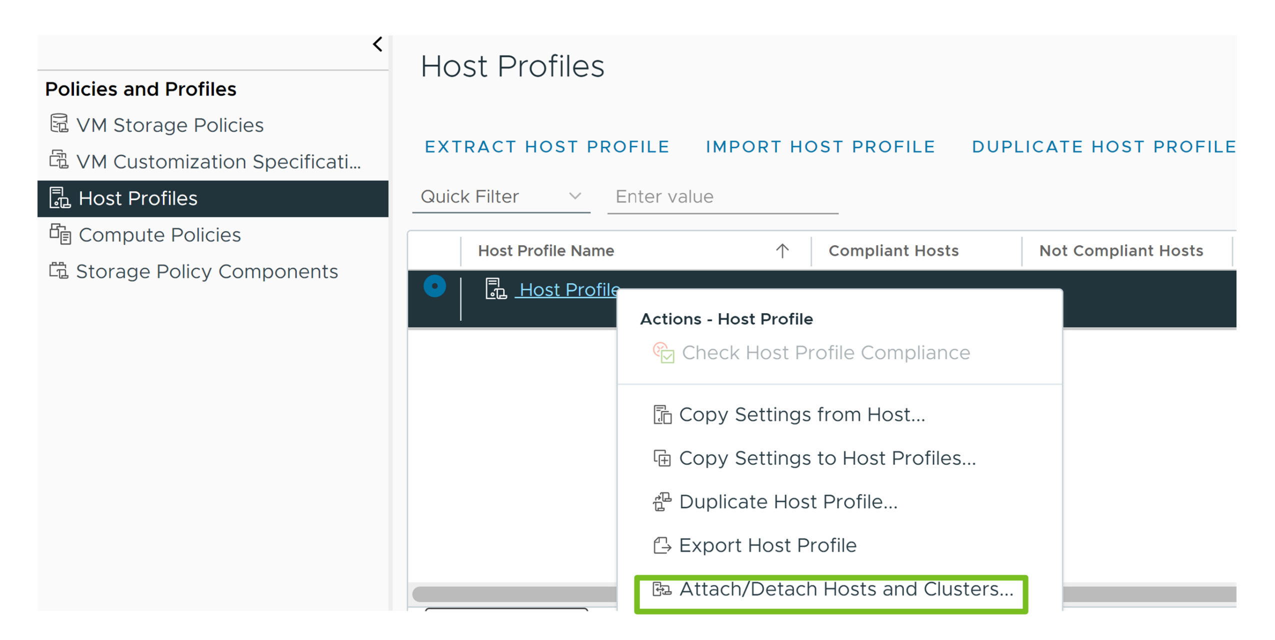
Note When vSphere Configuration Profiles is enabled on a cluster, you cannot attach or edit host profiles in the cluster or in the hosts in that cluster. For more information on vSphere Configuration Profiles, see the *Managing Host and Cluster Lifecycle* guide.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Right-click the host profile and select **Attach/Detach Hosts and Clusters** .



4 Select or deselect the hosts or clusters from the list, and click **Save**.

You can use the **Filter** text box to search the hosts and clusters list.

Results

The hosts or clusters are added or removed from the selected host profile.

How Do You Duplicate a vSphere Host Profile?

A host profile duplicate is a copy of an existing host profile. When you create the duplicate, you enter a new name and description for it and the duplicate appears in the list of host profiles.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Right-click the host profile you want to duplicate and select **Duplicate Host Profile**.

4 Enter a different name and description for the duplicate host profile, and click **OK**.

Results

A clone of the host profile appears in the **Host Profiles** list.

How Do You Copy Settings from a Reference Host to a vSphere Host Profile?

If the configuration of the reference host changes, you can update the host profile so that it matches the reference host's new configuration. You can make changes to the reference host and then copy the changes to the host profile. Alternatively, you can edit the host profile to match the new reference host configuration.

After you create a host profile, you can make incremental updates to the profile. When making changes to a host profile, consider the benefits and limitations of the two methods:

- Make the configuration changes to a host and copy that host's settings to the profile. The settings within the existing profile are updated to match those of the host. This method allows you to validate the configuration on a single host before rolling it to the other hosts that are attached to the profile.
- Update the profile directly by editing the host profile. This provides the ability to do more comprehensive and immediate remediation of those changes.

Note Fixed user password, system image cache and some of the host customized settings are not present in the newly updated host profile. Edit the host profile to update these settings.

Procedure

1. In the vSphere Client, select **Menu > Policies and Profiles**.
2. Under **Policies and Profiles**, click **Host Profiles**.
3. Right-click the host profile and click **Copy Settings from Host**.
4. Select the host from which you want to copy the configuration settings and click **OK**.

How Do You Import or Export a vSphere Host Profile?

You can import a host profile from a file that is in the VMware profile format (`.vpf`). You can also export a host profile to a file that is in the VMware profile format (`.vpf`).

When you export a host profile, administrator and user profile passwords are not exported. This is a security measure and stops passwords from being exported in plain text when the profile is exported. You are prompted to re-enter the values for the password after the profile is imported and the password is applied to a host.

Procedure

1. In the vSphere Client, select **Menu > Policies and Profiles**.
2. Under **Policies and Profiles**, click **Host Profiles**.
3. If you want to import a host profile, click **Import Host Profile**.
   a. To locate the VMware Profile Format file (`.vpf`) that you want to import, click **Browse**.
   b. Enter the **Name** and **Description** for the imported Host Profile, and click **OK**.

      The imported host profile appears in the **Host Profiles** list.
4. If you want to export a host profile, right-click the profile, select **Export Host Profile**, and click **Save**.

How Do You Copy Settings from a vSphere Host Profile?

After you make changes to a host profile, you can propagate those changes to other host profiles in the inventory.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Right-click the host profile from which you want to copy settings and select **Copy Settings to Host Profiles**.

4 Select the settings you want to copy to other host profiles, and click **Next**.

5 Select the target host profile that will be overwritten with the selected settings, and click **Next**.

   The differences between the host profile settings are displayed on the **Ready to complete** page.

6 Click **Finish**.

How Do You Manage Compliance Checks of Hosts and Clusters to a vSphere Host Profile

You can check the compliance of hosts and clusters to a vSphere host profile to verify if the host configuration matches the configuration of the host profile. Learn how to check compliance manually or schedule regular compliance checks of hosts and clusters, and how to remediate hosts that are not compliant with the host profile configuration.

How Do You Check Compliance of Hosts or Clusters to a vSphere Host Profile?

Learn how to check the compliance of a host or cluster to the host profile attached to them. By using the compliance check, you can see if any configuration parameters on a host are different from those specified in the host profile.

As a result of the compliance check, the host status is labeled as Compliant, Unknown, or Non-compliant.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Right-click a host profile and click **Check Host Profile Compliance**.

> **Note** Host profiles do not capture offline or unpresented devices. Any changes made to offline devices after extracting a host profile do not make a difference to the compliance check results.

Results

The compliance status is updated as Compliant, Unknown, or Non-compliant.

A non-compliant status indicates a discovered and specific inconsistency between the profile and the host. To resolve this, you should remediate the host. Any unknown status indicates that the compliance of the host cannot be verified. To resolve the issue, remediate the host through the host profile. Often the compliance check fails because the host is disconnected.

During a compliance check of an ESXi host to the host profile, two groups of advanced option parameters are not managed by the host profile and their values remain unchanged for the host:

- advanced option parameters which are disabled in the host profile.
- advanced option parameters which exist in the ESXi host you want to remediate, and do not exist in the host profile.

What to do next

To see more details on compliance failures, select a host profile from the **Host Profiles** main view for which the last compliance check displayed one or more failures. To see which parameters differ between the host that failed compliance and the host profile, click the **Monitor** tab and select the **Compliance** view. Then select the failing host. The differing parameters are displayed in the Compliance window, below the host list.

How Do You Schedule a Compliance Check of Hosts or Clusters to a vSphere Host Profile?

You can schedule a regular compliance check of a host or cluster, using a standard vSphere Client scheduled tasks workflow. This automation determines whether any configuration parameters are different from those specified in the host profile.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Select the desired host profile and navigate to the **Monitor** tab.

4 From the **Monitor** tab, select **Scheduled Tasks** -> **New Scheduled Task** -> **Check Compliance**.

   The **Schedule New Tasks (Check Compliance)** dialog box appears.

5 (Optional) Enter a new task name.

   Additional details about the task can be entered in the **Description** text box.

6 Choose a frequency how often to run the task.

   You can postpone when the task is run for the first time and schedule when it ends.

7 (Optional) To receive a notification after the task is finished, enter an email.

8 Click **Schedule The Task**.

Results

The newly created task is visible on the **Scheduled Tasks** list. You can **Edit**, **Run** or **Remove** the task.

What to do next

To understand more about compliance status, checks or failures, see **Check Compliance**.

How Do You Remediate a Host to Comply with a vSphere Host Profile Configuration?

When you check the compliance of a host to a host profile and a host is non-compliant, you can use the remediate option to apply the host profile settings to the host. During remediation, all host profile parameters are updated to the values defined in the host profile that is attached to the host.

Prerequisites

Verify that a host profile is attached to the host.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Right-click the host profile and select **Remediate**.

   Note Certain Host Profile policy configurations require that the host is rebooted after remediation. In such cases, you are prompted to place the host into maintenance mode. You might be required to place hosts into maintenance mode before remediation. Hosts that are in a fully automated DRS cluster are placed into maintenance mode during remediation. Alternatively, if the host is not placed into maintenance mode when required, the remediation process stops.

4 Select the hosts you want to remediate against the host profile.

Note When you remediate an ESXi host to comply with a host profile, two groups of advanced option parameters are not managed by the host profile and their values remain unchanged for the host:

- advanced option parameters which are disabled in the host profile.
- advanced option parameters which exist in the ESXi host you want to remediate, and do not exist in the host profile.

The remediation pre-check results do not contain tasks related to these two groups of advanced option parameters.

5 (Optional) To specify host properties, enter your host customizations or import a host customization file.

You can modify the user input parameters for the host profiles policies by customizing the host and clicking **Next**. See Host Profiles and vSphere Auto Deploy for more information about vSphere Auto Deploy.

6 To check if the selected hosts can be remediated, click **Pre-check Remediation**.

The pre-check generates a list of tasks that will be performed on the host.

7 If needed, select the check box to reboot the hosts.

Alternatively you can reboot the hosts manually after the remediation process.

8 Review the tasks that are necessary to remediate the host profile and click **Finish**.

Results

The compliance status is updated.

How Do You Configure vSphere Host Profiles

3

Learn how to edit host profile policies and components, and configure security and networking host profiles.

Read the following topics next:

How Do You Manage Host Profile Policies and Policy Components

In the vSphere Client, you can view and edit host profiles policies, policy options, and parameters. You can change policy names or policy descriptions. If you do not want a host profile component to be considered during a compliance check, you can deactivate that specific component.

How Do You Edit a vSphere Host Profile?

Learn how to view and change the host profile policy names and descriptions, how to mark specific configurations as favorite, and how to search for a specific configuration value.

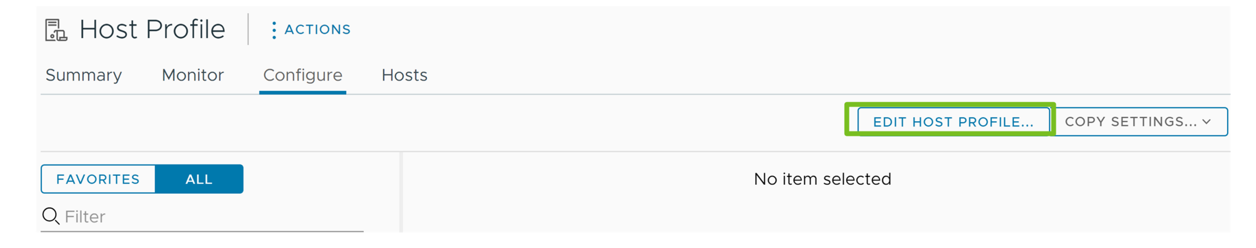
Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Select the host profile that you want to edit and click the **Configure** tab.

4 Click **Edit Host Profile**.



5 (Optional) To change the profile name and description, click the **Name and description** tab.

6 To view or edit a particular policy or settings, expand the category in the **Edit host profile** page.

Note See How Do You Edit a vSphere Host Profile Policy? for detailed instructions for editing a Host Profile policy. See How Do You Deactivate a Host Profile Component or Subprofile? for detailed instructions on enabling or disabling a policy from compliance check or remediation.

7 View **All** host profile configurations or only **Favorites** configurations.

You can mark a configuration as a favorite with the star icon. The configurations are then added to **Favorites** configurations.

8 (Optional) In the search field, filter the configuration names and values you want to view.

For example, enter **`SNMP`**. All configurations that relate to **SNMP** are displayed.

9 (Optional) Customize the hosts.

Make any changes to the available configuration values for this profile and click **Save**.

Note The host customization settings page only appears if you changed any settings that require host customizations.

Results

The changes are complete when the "Update Host Profile" task is completed in the **Recent Tasks** pane. If you attempt to remediate the profile before the task is complete, the profile configuration does not contain the change.

How Do You Edit a vSphere Host Profile Policy?

A host profile policy describes how a specific configuration setting is applied. You can edit policies belonging to a specific host profile.

To see the sub-profile components that comprise the host profile, you can expand the host profile's configuration hierarchy when you edit the host profile. These components are categorized by functional group or resource class to make it easier to find a particular parameter. Each subprofile component contains one or more attributes and parameters, with the policies and compliance checks.

Each policy consists of one or more options that contain one or more parameters. Each parameter consists of a key and a value. The value can be one of a few basic types, for example, integer, string, string array, or integer array.

Note Currently, there is no way to remove or replace policy options, policies, or sub-profiles that are deprecated in this release. To allow old host profiles to continue working, metadata is added to the deprecated policies. New host profiles are extracted with only non-deprecated parts of a host profile.

Table 3-1. Subset of Host Profile Subprofile Configurations

Component Categories	Configuration Settings	Notes and Examples
Advanced Configuration Settings	Advanced Options, Agent VM, DirectPath I/O, Hosts file, Power System, System Image Cache.	■ Host profiles do not check advanced settings if they are the same as the default settings. vCenter Server copies only the advanced configuration settings that have changed and that differ from the default values. In addition, compliance checks are limited to the settings that are copied. ■ Host profiles do not support the configuration of PCI devices for virtual machine passthrough on the ESXi host.
General System Settings	Console, Core Dump, Device Alias, Host Cache, Kernel Module, Management Agent, System Resource Pool, System Swap, vFlash Host Swap Cache, CIM-XML Indication Subscriptions.	For date and time configuration: ■ For the time zone, enter a UTC string. For example, "America/Los_Angeles" for United States Pacific time zone. ■ The default time zone is set to the local time and location of the vSphere Client machine. ■ Configure the Network Time Protocol (NTP) correctly. You can configure the NTP settings on the host **Configure** tab. Click **Time Configuration** (under System). To configure the time settings, click **Edit**. **Note** Enter the host cache size as a whole GB in MB. For example, 1024MB.
Networking	vSwitch, Port groups, Physical NIC speed, security and NIC teaming policies, vSphere Distributed Switch, and vSphere Distributed Switch uplink port.	When DHCPv6 is enabled in the networking subprofile, manually turn on the corresponding rule set in the firewall subprofile.

Table 3-1. Subset of Host Profile Subprofile Configurations (continued)

Component Categories	Configuration Settings	Notes and Examples
Security	Firewall, Security Settings, Service.	
Storage	Configure storage options, including Native Multi-Pathing (NMP), Pluggable Storage Architecture (PSA), iSCSI adapters, and NFS storage.	■ Use the vSphere CLI to configure or modify the NMP and PSA policies on a reference host, and then extract the Host Profile from that host. If you use the Profile Editor to edit the policies, to avoid compliance failures, make sure that you understand interrelationships between the NMP and PSA policies and the consequences of changing individual policies. For information about the NMP and PSA, see the *vSphere Storage* documentation. ■ Add the rules that change device attributes before extracting the Host Profile from the reference host. After attaching a host to the Host Profile, if you edit the profile and change the device attributes (for example, mask device paths or adding SATP rules to mark the device as SSD) you are prompted to reboot the host to make the changes. However, after rebooting, compliance failures occur because the attributes changed. Because Host Profiles extract device attributes before rebooting, if any changes occur after the reboot, it evaluates and finds those changes, and reports it as noncompliant. ■ To configure or modify the SatpDeviceProfile policy after extracting the host profile, use the vSphere Client. For compliance purposes, the policy option strings must be in the following format: ■ For an ALUA supported array, for example, SATP_ALUA, the policy options must be separated by a semicolon (;). For example: **`implicit_support=<on/off>; explicit_support=<on/off>; action_onRetryErrors=<on/off>`** ■ For an ALUA supported array with CX, for example, SATP_ALUA_CX, the policy options must be separated by a semicolon (;).

Table 3-1. Subset of Host Profile Subprofile Configurations (continued)

Component Categories	Configuration Settings	Notes and Examples
		For example: **navireg=<on/off>; implicit_support=<on/off>; action_onRetryErrors=<on/off>** ■ For a CX array, for example, SATP_CX or SATP_INV, the policy options must be separated by a space. For example: **navireg=<on/off> ipfilter=<on/off> action_onRetryErrors=<on/off>** **Note** The policy configuration options that are marked with **off** are not present in the configuration string.

Other profile configuration categories include: user group, authentication, kernel module, DCUI keyboard, host cache settings, SFCB, resource pools, login banner, SNMP agent, power system, and CIM indication subscriptions.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Select the host profile that you want to edit and click the **Configure** tab.

4 Click **Edit Host Profile**.

5 Expand a subprofile until you reach the policy to edit.

6 Select the policy.

The policy options and parameters appear on the right side of the **Edit Host Profile** dialog box.

7 Edit the policy options or parameters.

How Do You Deactivate a Host Profile Component or Subprofile?

You can decide whether a host profile component or a subprofile is applied or considered during a compliance check. This action allows administrators to eliminate non-critical attributes from consideration during the compliance check or ignore values that, while part of the host profile, are likely to vary between hosts.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Select the host profile that you want to edit and click the **Configure** tab.

4 Click **Edit Host Profile**.

5 Expand the Host Profile Component hierarchy until you reach the desired component or component element.

6 Deselect the check box next to a component.

The check box is selected by default. If you deselect the check box, the other subprofiles that are enabled are still applied and selected.

Results

During a host profile compliance check or host remediation, the component or component element is not considered.

Note Sometimes, deselecting the check box might remove the component or component element from the host. This action is displayed in the task list after the pre-check remediation.

How Do You Configure a Security vSphere Host Profile

Learn how to manage role profiles, user account profiles, lockdown mode profiles, and active directory permission profiles that are grouped as part of the security host profile. Starting with vSphere 8.0, users with access to the ESXi Shell and the Administrator role can remove or grant ESXi Shell access to user accounts.

You can configure the host profile options, part of the security profile.

Prerequisites

Make sure that you have the SecurityConfigProfile plugin available to validate the role, user account, and active directory permission profiles as there are dependencies between them.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Select the host profile that you want to edit and click the **Configure** tab.

4 Click **Edit Host Profile**.

5 Unfold the **Security and Services** > **Security Settings** profile category and open the **Security** folder.

The following profiles are displayed:

Role	This profile allows you to view default roles and add custom roles within the ESXi system.
User Configuration	This profile allows you to create and manage user accounts. By default, newly created user accounts have access to the ESXi Shell. Starting with vSphere 8.0, administrators can use the advanced option `Security.DefaultShellAccess` to change this default behavior. Here are some of the operations that you can perform for user accounts: ■ Create a user account. ■ Configure the password for a user account. ■ Configure the password for the root user. ■ Activate or deactivate user account ESXi Shell access. **Note** Do not modify the shell access property for the root user account. ■ Configure the role for any user that is not the default one. ■ Assign a default or a custom role (configure permissions) for a local account. ■ Configure the SSH key for any user.
Active Directory Permission	This profile allows you to manage permissions for active directory users or groups. For example, you can create permissions that associate an active directory user or a group with a role. When an ESXi host joins the active directory domain, an Admin permission is created for the DOMAIN group **ESX Admins**. Also, when an active directory user or group is given some permissions on the ESXi host, a corresponding permission is created on that host. The Active Directory Permission profile captures that permission.
Lockdown Mode	This profile allows you to increase the security of your ESXi hosts by restricting user permissions and privileges. You can configure the following lockdown mode settings: ■ Normal lockdown mode: An ESXi host can be accessed from a local console and vCenter Server. DCUI service is not stopped. ■ Strict lockdown mode: An ESXi host can be only accessed from vCenter Server. The DCUI service is stopped. ■ Exception users: The users that still have their permissions regardless of the lockdown mode state.

For more information on the security profile, see the *vSphere Security* documentation.

How Do You Configure a Networking vSphere Host Profile

By default, hosts provisioned with vSphere Auto Deploy are assigned DHCP addresses by a DHCP server. You can use the vSphere Auto Deploy host customization mechanism to assign static IP addresses to hosts.

Prerequisites

- Set up your vSphere Auto Deploy environment.
- Boot the host using vSphere Auto Deploy.
- Extract a host profile from the host.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Select the host profile that you want to edit and click the **Configure** tab.

4 Click **Edit Host Profile**.

5 Change the default IP address settings by locating **Networking configuration** > **Host port group** > **Management Network** > **IP address settings**.

6 From the **IPv4 address** drop-down menu, select **User specified IP address to be used while applying the configuration**.

7 If the host is in a different subnet than the vCenter Server system, select **Networking Configuration** > **NetStack Instance** > **defaultTcpipStack** > **DNS configuration** and enter the default route in the **Default IPv4 gateway** text box.

8 Select **Networking Configuration** > **NetStack Instance** > **defaultTcpipStack** > **DNS configuration**.

9 Make sure the **Flag indicating if DHCP should be used** check box is deselected.

10 Right-click the host and select **All vCenter Actions** > **Host Profiles** > **Attach Host Profile**.

11 Select the profile to attach, and click **Next**.

12 Provide the IP address and net mask, and click **Finish**.

13 Reboot the ESXi host.

Results

The IP address is saved as a host customization and applied to the host.

How Do You Customize Hosts by Using vSphere Host Profiles

4

To customize hosts with shared attributes, you can create a host profile in a reference host. To customize individual hosts, you can set up some fields in the host profile to prompt the user for input for each host. You can also edit and export host customizations.

Host Customization

Host profiles allow you to prespecify information, for example, the storage setup or Syslog setup in a reference host to and apply the host profile to a set of target hosts that share the same settings. You can also use host profiles to specify that certain settings are host dependent. If you do so, the host comes up in maintenance mode when you provision it with Auto Deploy. Remediate the host or reset the host customization to be prompted for input. The system stores your input and uses it the next time the host boots.

When the host profile is set to prompt for user input, you must specify a value in the dialog box that appears when you reset the host customization. An error results if you do not specify a value.

Table 4-1. Host Profile Options that Prompt for iSCSI User Input

Information to Request User Input For	Setting the Host Profile Option
When you apply a host profile on a system that includes a profile for iSCSI, you are prompted for several properties. For many of the properties, a system default is available. For some properties, you must specify a value or an error results. **IQN name** If the iSCSI setup uses an IQN name, you are prompted when you apply the host profile. You cannot continue until you provide the name. **CHAP information** If you set up iSCSI to require CHAP authentication, you are prompted for CHAP information including the user name and the secret when you apply the host profile. You cannot continue until you provide the name.	1 Select **Edit Host Profile**, click **Storage configuration**, and click **iSCSI Initiator Configuration**. 2 Select the folder for an already enabled initiator and set up the initiator. 3 Set up the initiator. For many fields, the user is prompted as part of host customization.

Table 4-2. Host Profile Options that Prompt for Storage User Input

Information to Request User Input For	Setting the Host Profile Option
You are setting up the Fixed PSP configuration and want to prompt for the adapter and target IDs for the storage arrays that should use the Fixed PSP.	You can set the option only if the adapter is set up to use the Fixed PSP. 1 Select **Edit Host Profile**, click **Storage configuration**. 2 Click **Native Multipathing (NMP)**. 3 Click **Path Selection Policy (PSP) configuration**. 4 In the Preferred Path window, select **Prompt the user for adapter and target IDs on the host**.

Table 4-3. Host Profile Options that Prompt for Security User Input

Information to Request User Input For	Setting the Host Profile Option
Administrator password for ESXi host when the host boots for the first time.	1 Select **Edit Host Profile**, and click **Security and Services**. 2 click **Security Settings** and click **Security configuration**. 3 In the right panel, select **User Input Password to be Used to Configure Administrator Password** from the **Administrator password** drop-down menu.
Preconfigures a user for the ESXi host but prompts for the password for that user on each host when the host boots for the first time.	You can perform this task only if a user configuration already exists. Configure the user by selecting one of the options. ■ **Assigned fixed user configurations** is available for compatibility with ESX/ESXi 4.1 system, this option displays the password in the clear. ■ **Assign advanced fixed user configurations** is for users of ESXi 5.0 and later systems. ■ **Specify the user configuration in the profile but prompt for password during host configuration** allows you to specify the information about the user but prompt for a password on each host.
Prompt the user for credentials when the host joins the Active Directory domain.	1 Set the Authentication configuration profile to use a fixed domain. a Select **Edit Host Profile**, click **Security and Services**. b Click **Security Settings**, and click **Authentication configuration**. c Click **Active Directory configuration**. d In the Domain Name drop-down menu, select **Configure a fixed domain name**. 2 Set the method for joining the domain to prompt the user. a Select **Edit Host Profile**, click **Security and Services** and click **Authentication configuration**. b Click **Active Directory configuration**. c In the Join Domain Method drop-down menu, select **Use user specified AD credentials to join the host to domain**.

Table 4-4. Host Profile Options that Prompt for Networking User Input

Information to Request User Input For	Setting the Host Profile Option
Prompt the user for the MAC address for a port group. You can have the system prompt the user in all cases (User specified MAC address...) or prompt the user only if no default is available.	1 Select **Edit Host Profile,** click **Networking configuration**, and click **Host port group**. 2 Click **Management Network**. 3 In the **Determine how MAC address for vmknic should be decided** field, select how the system manages the MAC address. ■ **User specified MAC Address to be used while applying the configuration** ■ **Prompt the user for the MAC Address if no default is available**
Prompt the user for the IPv4 address for each ESXi host to which the profile is applied. You can have the system prompt the user in all cases (User specified IPv4 address...) or prompt the user only if no default is available.	1 Select **Edit Host Profile,** click **Networking configuration**, and click **Host port group**. 2 Click **Management Network** and click **IP address settings**. 3 In the **IPv4 address** field, select how the system manages the IPv4 address. ■ **User specified IPv4 Address to be used while applying the configuration** ■ **Prompt the user for the IPv4 Address if no default is available**
Prompt the user for the IPv6 address for each ESXi host to which the profile is applied. You can have the system prompt the user in all cases (User specified IPv6 address...) or prompt the user only if no default is available.	1 Select **Edit Host Profile,** click **Networking configuration**, and click **Host port group**. 2 Click **Management Network** and click **IP address settings**. 3 In the **Static IPv6 address** field, select how the system manages the IPv6 address. ■ **User specified IPv6 Address to be used while applying the configuration** ■ **Prompt the user for the IPv6 Address if no default is available**
Prompt the user for the DNS name of the host. You can have the system prompt the user in all cases (User specified host name...) or prompt the user only if no default is available.	1 Select **Edit Host Profile,** click **Networking configuration**, and click **DNS configuration**. 2 In the Host name field, select how the system manages the DNS configuration. ■ **Prompt the user for host name if default is not available** ■ **User specified host name to be used while applying the configuration**

Table 4-4. Host Profile Options that Prompt for Networking User Input (continued)

Information to Request User Input For	Setting the Host Profile Option
Prompt the user for the MAC address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click the **Add sub-profile** icon to determine the component to which the setting is applied. You can decide to prompt the user in all cases or only if no default is available.	1 Open **Networking configuration**. 2 Click **Host virtual NIC**. 3 In the **Determine how MAC address for vmknic should be decided** field, select how the system manages the MAC address for the distributed switch. ■ **User specified MAC address to be used while applying the configuration** ■ **Prompt the user for the MAC address if no default is available**
Prompt the user for the IPv4 address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click the **Add sub-profile** icon to determine the component to which the setting is applied. You can decide to prompt the user only if no default is available or in all cases.	1 Open **Networking configuration**. 2 Click **Host virtual NIC**. 3 Click **IP address settings**. 4 In the IPv4 address field, select how the system handles the IPv4 address for the distributed switch. ■ **User specified IPv4 address to be used while applying the configuration** ■ **Prompt the user for IPv4 address if no default is available**
Prompt the user for the IPv6 address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click the **Add sub-profile** icon to determine the component to which the setting is applied. You can decide to prompt the user only if no default is available or in all cases.	1 Open **Networking configuration**. 2 Open **Host virtual NIC**. 3 Open **IP address settings**. 4 In the **Static IPv6 address** field, select how the system manages the IPv6 address for the distributed switch. ■ **User specified IPv6 address to be used while applying the configuration** ■ **Prompt the user for IPv6 address if no default is available**

Read the following topics next:

- How Do You Export Host Customizations?
- How Do You Edit Host Customizations?
- Answer File Field and vSphere Host Profile Extraction

How Do You Export Host Customizations?

Learn how to export the customized attributes of a vSphere host profile as a `.CSV` file to your desktop.

For security reasons, sensitive data such as passwords are not exported.

Procedure

1 Navigate to **Hosts and Clusters** and select an ESXi host with an attached host profile.

2 Right-click the ESXi host and select **Host Profiles > Export Host Customizations**.

3 Click **Save**.

Note Only an English version of the `.csv` file is supported.

The file is saved as a `.csv` file.

What to do next

After the file is saved to your desktop, you can manually edit the file and save it to apply the customizations later.

How Do You Edit Host Customizations?

Read how to edit host customizations for specific hosts attached to a vSphere host profile or a cluster attached to a host profile.

Procedure

1 In the vSphere Client, select **Menu > Policies and Profiles**.

2 Under **Policies and Profiles**, click **Host Profiles**.

3 Right-click the host profile and select **Edit Host Customizations**.

4 Select the host or hosts for which you want to edit the customization, and click **Next**.

5 (Optional) To import host customization from your desktop, you can select **Import Host Customization** `.csv` in the **Customize hosts** page.

If you want to edit host customizations by using a `.csv` file, you can export the host customizations in `.csv` file format, edit the values in the answer file fields, and then import the file. For more information on how to export host customizations, see How Do You Export Host Customizations?.

Note User input in the **Customize hosts** pane is overwritten by the import process and the values from the `.csv` file.

After importing the `.csv` file, the text boxes are updated with the information from the file.

6 Edit the host configuration values and click **Finish**.

Answer File Field and vSphere Host Profile Extraction

When a new profile is extracted from an ESXi host or post upgrade, host profiles policy options and host customization values are changed. You can get more familiar with the changes by referring to the Answer File Field and Host Profile Extraction table.

After you extract a new host profile from an ESXi host, the values for some of the policy options change. To keep these values, you have to save them manually before extracting the host profile. The *Answer File Field and Host Profile Extraction* table lists the policy options with changed values and the options that keep their values the same in the newly extracted host profile.

To locate the policy options, navigate to **Host Profiles** main view, right-click the extracted host profile, and select **Edit Host Customizations.**

Table 4-5. Answer File Field and Host Profile Extraction

Policy option path	Policy option	Variations in the policy options value in the newly extracted profile
Security and Services -> Security Settings -> Security	`UserInputPasswordConfigOption`	For default users, it leaves the password unchanged (root). For non-default users, it always extracts user input.
	`UserInputPasswordConfigOption`	If host profile version is earlier than 6.5, this option is not extracted. You explicitly need to create a UserAccount profile in the extracted host profile.
	`UserInputAdminPasswordOption`	Changes to fixed. Does not keep user input value.
Storage configuration -> iSCSI Initiator Configuration	`AdvancedUserInputUserConfigOption`	Changes to fixed. Does not keep user input value.
	`UserInputIqn`	Keeps user input value.
	`UserInputAlias`	Keeps user input value.
	`UserInputChapName`	Changes to fixed. Does not keep user input value.
	`UserInputChapSecret`	Changes to fixed. Does not keep user input value.
	`UserInputFirstBurstLength`	Changes to fixed. Does not keep user input value.
	`UserInputMaxBurstLength`	Changes to fixed. Does not keep user input value.
General System Settings -> Management Agent Configuration -> SNMP Agent Configuration	`UserInputMaxReceiveSegmentLength`	Changes to fixed. Does not keep user input value.
	`UserInputUsers`	Changes to fixed. Does not keep user input value.
	`UserInputV3Targets`	Changes to fixed. Does not keep user input value.
	`UserInputEngineId`	Changes to fixed. Does not keep user input value.
	`UserInputContact`	Changes to fixed. Does not keep user input value.
	`UserInputLocation`	Changes to fixed. Does not keep user input value.
Security and Services -> Security Settings -> Security -> Active Directory Permission	`UserInputUserName`	Keeps user input value.
	`UserInputPassword`	Keeps user input value.
Networking Configuration	`UserInputMacAddress`	Conditional, prompt user if no default value is available.
	`UserInputHostName`	Conditional, prompt user if no default value is available.
	`UserInputIPAddress`	Conditional, prompt user if no default value is available.

Table 4-5. Answer File Field and Host Profile Extraction (continued)

Policy option path	Policy option	Variations in the policy options value in the newly extracted profile
Advanced Configuration Settings -> Advanced Options	`UserInputAdvancedConfigOption`	Changes to fixed. Does not keep user input value.
Advanced Configuration Settings -> System Image Cache Configuration	`Enable Stateless Caching`	You must explicitly select the policy option.
	`Enable Stateful Install`	You must explicitly select the policy option.

Note This table does not list all policy options. You must be aware of the policy options you modified before extracting a new host profile.

Recommended Upgrade Workflows for vSphere Host Profiles

5

Each workflow is the recommended upgrade path while upgrading your vCenter Server 6.5, 6.7 and 7.0 environment, that contains one or more host profiles with version 6.5, 6.7 and 7.0.

Upgrade Support Matrix

When you upgrade your vCenter Server from version 6.7 or 7.0 to version 8.0, you can keep your current ESXi host version and host profiles version. To ensure the best possible performance, when you upgrade the ESXi host, also upgrade the host profile. The host profile version must match the ESXi host version.

Note vCenter Server instances and ESXi hosts of versions 6.5 or earlier are not supported in vCenter Server 8.0. You can use the *Recommended Host Profiles Upgrade Workflows* in the *vSphere Host Profiles 6.7* guide as intermediate upgrade steps.

Table 5-1. Upgrade Support Matrix

Upgrade Workflow	vCenter Server	ESXi host	Host Profiles
earlier than 6.5 → 7.0 **Note** You must first upgrade your vCenter Server and ESXi hosts to versions 6.5 or 6.7. You can use the *Recommended Host Profiles Upgrade Workflows* in the *vSphere Host Profiles 6.7* guide as intermediate upgrade steps.	Requires an upgrade	Requires an upgrade	Requires an upgrade
6.5 → 7.0	Requires an upgrade	An optional upgrade	An optional upgrade
6.7 → 7.0	Requires an upgrade	An optional upgrade	An optional upgrade
6.5/6.7/7.0 → 7.0 Update 3 **Note** If you want to validate or edit a 7.0 GA host profile, you might need to keep an ESXi host of version 7.0 GA.	Requires an upgrade	An optional upgrade	An optional upgrade

Table 5-1. Upgrade Support Matrix (continued)

Upgrade Workflow	vCenter Server	ESXi host	Host Profiles
6.5 → 8.0 **Note** You must first upgrade your vCenter Server and ESXi hosts to versions 6.7 or 7.0. You can use the *Recommended Host Profiles Upgrade Workflows* in the *vSphere Host Profiles 7.0* guide as intermediate upgrade steps.	Requires an upgrade	Requires an upgrade	Requires an upgrade
6.7/7.0 → 8.0	Requires an upgrade	An optional upgrade	An optional upgrade

vCenter Server and ESXi Version Interoperability

Starting with vSphere 7.0 Update 3, a major-version vCenter Server instance supports any ESXi Update release version of the corresponding major release. That is, a vCenter Server 8.0 instance can manage ESXi 6.7, ESXi 7.0, ESXi 8.0, and any Update release of ESXi 8.0.

For more information about vCenter Server and ESXi Version Interoperability, you can refer to the VMware Product Interoperability Matrix.

Read the following topics next:

- How Do You Upgrade Host Profiles and vCenter Server from 6.5 to 8.0
- How Do You Upgrade vSphere Host Profiles and vCenter Server from 6.7 to 8.0
- How Do You Upgrade vSphere Host Profiles and vCenter Server from 7.0 to 8.0
- Using vSphere Host Profiles to Migrate an NSX Virtual Distributed Switch to a vSphere Distributed Switch

How Do You Upgrade Host Profiles and vCenter Server from 6.5 to 8.0

Use the upgrade workflows to resolve version compliance errors when upgrading vCenter Server with version 6.5 to version 8.0.

ESXi hosts of versions 5.5 and 6.0 are not supported in vCenter Server 8.0. You can use the *Recommended Host Profiles Upgrade Workflows* in the *vSphere Host Profiles 6.7* guide as intermediate upgrade steps.

How Do You Upgrade Host Profiles in a vCenter Server Instance with Stateful ESXi 6.5 Hosts Only?

You can use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.5 to version 8.0, if your cluster contains stateful ESXi 6.5 hosts.

Prerequisites

- Verify that your cluster contains ESXi 6.5 hosts only.
- Verify that a host profile with version 6.5 is attached to the cluster.
- Verify that your vCenter Server is with version 6.5.

Procedure

1. Upgrade all ESXi hosts in the cluster to version 7.0.

   For more information, see the *VMware ESXi Upgrade* documentation.

2. Remediate the upgraded hosts against the host profile with version 6.5.

   During remediation, all host profile settings are applied to the hosts in the cluster.

3. Extract a new host profile from an ESXi 7.0 host in the cluster.

   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

4. Attach the host profile with version 7.0 to the cluster.
5. Remediate the cluster against the host profile with version 7.0.
6. Upgrade your vCenter Server instance to version 8.0.

   The vCenter Server configuration is not changed during the upgrade.

   For more information, see the *vCenter Server Upgrade* documentation.

7. Upgrade all ESXi hosts in the cluster to version 8.0.

   Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534

8. Remediate the cluster against the host profile with version 7.0.

   During remediation, all host profile settings are applied.

9. Extract a new host profile from an ESXi 8.0 host.

   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

10. Attach the host profile with version 8.0 to the cluster.

    Edit host customization to validate host customization data.

    All host profile operations become available.

How Do You Upgrade Host Profiles in a vCenter Server Instance with Stateless ESXi 6.5 Hosts Only?

You can use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.5 to version 8.0, if your cluster contains stateless ESXi 6.5 hosts.

Prerequisites

- Verify that your cluster contains ESXi 6.5 hosts only.
- Verify that a host profile with version 6.5 is attached to the cluster.
- Verify that your vCenter Server is with version 6.5.

Procedure

1 Upgrade your vCenter Server instance to version 7.0.

   The vCenter Server configuration is not changed during the upgrade.

   For more information, see the *vCenter Server Upgrade* documentation.

2 Create a new rule or edit the existing rule with an image profile version 7.0 and select the cluster.

3 Remediate all ESXi hosts in the cluster by clicking **Remediate Host Associations**.

4 Reboot all ESXi hosts in the cluster.

   All hosts are compliant with the host profile version 6.5, but the host profile cannot be edited. Remediation and check compliance operations are available.

5 To be able to customize your host profile, follow these steps.

   a Extract a new host profile from an ESXi 7.0 host.

      During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

   b Attach the host profile with version 7.0 to the cluster.

      Edit host customization to validate host customization data.

      All host profile operations become available.

6 Upgrade your vCenter Server instance to version 8.0.

   The vCenter Server configuration is not changed during the upgrade.

   For more information, see the *vCenter Server Upgrade* documentation.

7 Create a new rule or edit the existing rule with an image profile version 8.0 and select the cluster.

8 Remediate all ESXi hosts in the cluster by clicking **Remediate Host Associations**.

9 Reboot all ESXi hosts in the cluster.

   All hosts are compliant with the host profile version 6.5, but the host profile cannot be edited. Remediation and check compliance operations are available.

10 To be able to customize your host profile, follow these steps.

  a Extract a new host profile from an ESXi 8.0 host.

    During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

  b Attach the host profile with version 8.0 to the cluster.

    Edit host customization to validate host customization data.

    All host profile operations become available.

How Do You Upgrade vSphere Host Profiles and vCenter Server from 6.7 to 8.0

Use the upgrade workflows to resolve version compliance errors when upgrading vCenter Server with version 6.7 to version 8.0.

How Do You Upgrade Host Profiles in a vCenter Server Instance with Stateful ESXi 6.5 and 6.7 Hosts?

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.7 to version 8.0, if your cluster contains stateful ESXi 6.5 and 6.7 hosts.

Prerequisites

- Verify that your cluster contains ESXi 6.5 and ESXi 6.7 hosts.
- Verify that a host profile with version 6.5 is attached to the cluster.
- Verify that your vCenter Server is with version 6.7.
- Upgrade all ESXi hosts and host profiles of version 6.5 to version 6.7.

  You can use the *Recommended Host Profiles Upgrade Workflows* in the *vSphere Host Profiles 6.7* guide as intermediate upgrade steps.

Procedure

1 Upgrade your vCenter Server instance to version 8.0.

  The vCenter Server configuration is not changed during the upgrade.

  For more information, see the *vCenter Server Upgrade* documentation.

2 Upgrade all ESXi hosts in the cluster to version 8.0.

  Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534

3 Remediate the cluster against the host profile with version 6.7.

  During remediation, all host profile settings are applied.

4 Extract a new host profile from an ESXi 8.0 host.

During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

5 Attach the host profile with version 8.0 to the cluster.

The host customization data updates automatically.

All host profile operations become available.

How Do You Upgrade Host Profiles in a vCenter Server Instance with Stateful ESXi 6.7 Hosts Only?

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.7 to version 8.0, if your cluster contains stateful ESXi 6.7 hosts.

Prerequisites

- Verify that your cluster contains ESXi 6.7 hosts only.
- Verify that a host profile with version 6.7 is attached to the cluster.
- Verify that your vCenter Server is with version 6.7.

Procedure

1 Upgrade your vCenter Server instance to version 8.0.

The vCenter Server configuration is not changed during the upgrade.

For more information, see the *vCenter Server Upgrade* documentation.

2 Upgrade all ESXi hosts in the cluster to version 8.0.

Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534

3 Remediate the cluster against the host profile with version 6.7.

During remediation, all host profile settings are applied.

4 Extract a new host profile from an ESXi 8.0 host.

During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

5 Attach the host profile with version 8.0 to the cluster.

The host customization data updates automatically.

All host profile operations become available.

How Do You Upgrade Host Profiles in a vCenter Server Instance with Stateless ESXi 6.7 Hosts Only?

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.7 to version 8.0, if your cluster contains stateless ESXi 6.7 hosts.

Prerequisites

- Verify that your cluster contains ESXi 6.7 hosts only.
- Verify that a host profile with version 6.7 is attached to the cluster.
- Verify that your vCenter Server is with version 6.7.

Procedure

1 Upgrade your vCenter Server instance to version 8.0.

   The vCenter Server configuration is not changed during the upgrade.

   For more information, see the *vCenter Server Upgrade* documentation.

2 Create a new rule or edit the existing rule with an image profile version 8.0 and select the cluster.

3 Remediate all ESXi hosts in the cluster by clicking **Remediate Host Associations**.

4 Reboot all ESXi hosts in the cluster.

   All hosts are compliant with the host profile version 6.7, but the host profile cannot be edited. Remediation and check compliance operations are available.

What to do next

To be able to customize your host profile, follow these steps.

1 Extract a new host profile from an ESXi 8.0 host.

   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

2 Attach the host profile with version 8.0 to the cluster.

   The host customization data updates automatically.

   All host profile operations become available.

How Do You Upgrade vSphere Host Profiles and vCenter Server from 7.0 to 8.0

Use the upgrade workflows to resolve version compliance errors when upgrading vCenter Server with version 7.0 to version 8.0.

How Do You Upgrade Host Profiles in a vCenter Server Instance with Stateful ESXi Hosts of version 6.7 and 7.0?

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 7.0 to version 8.0, if your cluster contains stateful ESXi 6.7 and 7.0 hosts.

Prerequisites

- Verify that your cluster contains ESXi 6.7 and ESXi 7.0 hosts.
- Verify that a host profile with version 6.7 is attached to the cluster.
- Verify that your vCenter Server is with version 7.0.

Procedure

1 Upgrade your vCenter Server instance to version 8.0.

   The vCenter Server configuration is not changed during the upgrade.

   For more information, see the *vCenter Server Upgrade* documentation.

2 Upgrade all ESXi hosts in the cluster to version 8.0.

   Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534

3 Remediate the cluster against the host profile with version 6.7.

   During remediation, all host profile settings are applied.

4 Extract a new host profile from an ESXi 8.0 host.

   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

5 Attach the host profile with version 8.0 to the cluster.

   The host customization data updates automatically.

   All host profile operations become available.

How Do You Upgrade Host Profiles in a vCenter Server Instance with Stateful ESXi 7.0 Hosts Only?

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 7.0 to version 8.0, if your cluster contains stateful ESXi 7.0 hosts.

Prerequisites

- Verify that your cluster contains ESXi 7.0 hosts only.
- Verify that a host profile with version 7.0 is attached to the cluster.
- Verify that your vCenter Server is with version 7.0.

Procedure

1 Upgrade your vCenter Server instance to version 8.0.

The vCenter Server configuration is not changed during the upgrade.

For more information, see the *vCenter Server Upgrade* documentation.

2 Upgrade all ESXi hosts in the cluster to version 8.0.

Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534

3 Remediate the cluster against the host profile with version 7.0.

During remediation, all host profile settings are applied.

4 Extract a new host profile from an ESXi 8.0 host.

During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

5 Attach the host profile with version 8.0 to the cluster.

The host customization data updates automatically.

All host profile operations become available.

How Do You Upgrade Host Profiles in a vCenter Server Instance With Stateless ESXi 7.0 Hosts Only?

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 7.0 to version 8.0, if your cluster contains stateless ESXi 7.0 hosts.

Prerequisites

- Verify that your cluster contains ESXi 7.0 hosts only.
- Verify that a host profile with version 7.0 is attached to the cluster.
- Verify that your vCenter Server is with version 7.0.

Procedure

1 Upgrade your vCenter Server instance to version 8.0.

The vCenter Server configuration is not changed during the upgrade.

For more information, see the *vCenter Server Upgrade* documentation.

2 Create a new rule or edit the existing rule with an image profile version 8.0 and select the cluster.

3 Remediate all ESXi hosts in the cluster by clicking **Remediate Host Associations.**

4 Reboot all ESXi hosts in the cluster.

All hosts are compliant with the host profile version 7.0, but the host profile cannot be edited. Remediation and check compliance operations are available.

What to do next

To be able to customize your host profile, follow these steps.

1 Extract a new host profile from an ESXi 8.0 host.

During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and vSphere Host Profile Extraction.

2 Attach the host profile with version 8.0 to the cluster.

The host customization data updates automatically.

All host profile operations become available.

Using vSphere Host Profiles to Migrate an NSX Virtual Distributed Switch to a vSphere Distributed Switch

For clusters enabled with VMware NSX®, you can use the regular ESXi upgrade workflow to migrate the NSX-managed Virtual Distributed Switches of the hosts to vCenter Server-managed vSphere Distributed Switches. By using host profiles, you can perform the upgrade and the host switch migration in an environment where all hosts are provisioned with Auto Deploy.

Starting with vSphere 7.0, the vSphere Distributed Switch supports the NSX functionality. Migrating your host switch to vSphere Distributed Switch 7.0 ensures optimal pNIC usage, and lets you manage the networking for your NSX hosts from vCenter Server.

Requirements

- Verify that the ESXi hosts to upgrade are version 6.7 or later.
- vCenter Server 7.0 Update 2
- VMware NSX® 3.1.1

As a good practice, contact VMware support to assess the impact of migrating to vSphere Distributed Switch 7.0.

Workflow

1 Upgrade vCenter Server to version 7.0 Update 2.

For more information about upgrading vCenter Server, see the *vSphere Upgrade* documentation.

2 Upload a software depot that contains an ESXi 7.0 Update 2 image. to vCenter Server.

For more information, see the *VMware ESXi Installation and Setup* documentation.

3 In NSX Manager, run the migration readiness pre-check, address any configuration issues, review the recommended topology, and create a vSphere Distributed Switch.

Note At this point, do not make any configuration changes to VMware NSX®.

For more information about the steps you need to perform in NSX Manager, see "Migrate Host Switch to vSphere Distributed Switch" in the *NSX Administration* documentation.

4 Create a new image rule or update the existing one with the uploaded ESXi 7.0 Update 2 image.

For more information, see the *VMware ESXi Installation and Setup* documentation.

5 Reboot the reference host.

The reboot triggers the migration of the host switches from NSX Virtual Distributed Switches to vSphere Distributed Switches.

After the reboot, the ESXi version on the reference host is upgraded to 7.0 Update 2. A new TNP with vSphere Distributed Switch is attached to the cluster.

6 Update the host profile by copying the settings from the reference host.

The updated host profile is configured with vSphere Distributed Switch instead of NSX Virtual Distributed Switch.

For more information, see How Do You Copy Settings from a Reference Host to a vSphere Host Profile?.

7 Reboot all ESXi hosts in the cluster.

After the reboot, all hosts in the cluster use the new host profile, which is configured with vSphere Distributed Switch instead of NSX Virtual Distributed Switch.

Troubleshooting vSphere Host Profiles

6

The Host Profiles troubleshooting topics provide solutions to problems that you might encounter when performing tasks for vSphere Host Profiles in vCenter Server .

If upgrading your vCenter Server to version 8.0 results with a failure due to an existing host profile in the inventory, see *vCenter Server Upgrade* for Upgrade Issues with vCenter Server Containing Host Profiles.

Read the following topics next:

- Host Customization Data Is Missing
- Reference Host is Unavailable
- Compliance Failures with vSphere Storage Host Profiles
- Edit Settings for vSphere Host Profiles is Failing
- vSphere Host Profile without an NFS Datastore
- Upgraded Host is Not Compliant with a Legacy Host Profile

Host Customization Data Is Missing

Deploying a stateless host results with a failure in exiting maintenance mode.

Problem

When you are in the process of deploying a stateless host, the host fails in exiting maintenance mode.

Cause

In an environment where the following takes place for a host profile:

- The host profile is attached to a stateless host.
- The host profile has host-specific settings.

When the stateless host is rebooting, applying the host profile fails because the host does not exit from a maintenance mode.

Solution

- Provide a host customization as described in How Do You Edit Host Customizations?.
- Remediate the host profile to the host again.
- Reboot the host, if needed.
- Refer to the host profiles command-line utility in Host Profiles CLI for customizing stateless hosts.

Reference Host is Unavailable

Creating a vSphere Host Profile in the vCenter Server inventory results with a failure.

Problem

When you perform Host Profiles operations in the vCenter Server inventory such as:

- Edit a Host Profile.
- Import a Host Profile.
- Export a Host Profile.

The process of creating a host profile fails with an error.

```
There is no suitable host in the inventory as reference host for the profile Host Profile.
The profile does not have any associated reference host.
```

Cause

The vCenter Server inventory does not have a compatible host that acts as a reference host for the host profile you are trying to create.

Solution

- ◆ Add a host that acts as a reference host in the vCenter Server inventory with the same version as the host profile you are trying to create.

Compliance Failures with vSphere Storage Host Profiles

When you use storage devices, that are not shared across a cluster, but the vSphere storage stack cannot detect them as local (for example, some SAS devices), applying a host profile might result with compliance failures.

To resolve the compliance failures caused by using local storage devices, use the upgraded Pluggable Storage Architecture (PSA) host profile policies.

To find out whether a device is detected as local or not, you can check the **Is Local** setting for a device by running the command `esxcli storage core device list -d naa.xxxx` in the ESXi shell. For more information on this command and identifying disks or LUNs, see KB 1014953.

Note ESXi diagnostic data that you obtain by running the `vm-support` command contains host profiles information which includes storage host profiles, PSA, NMP, and Virtual Volumes data. No sensitive information, such as passwords, is collected.

Compliance Failures with Serial Attached SCSI (SAS) Devices

This procedure resolves compliance failures for SAS devices that are not detected as local by the vSphere storage stack.

Prerequisites

Extract a host profile from a reference host. See How Do You Create a vSphere Host Profile? for instructions.

Procedure

1 Navigate to **Host Profiles** main view and select the host profile that you want to edit.

2 Click the **Configure** tab, and click **Edit Host Profile**.

3 Select **Storage configuration > Pluggable Storage Architecture configuration > PSA device sharing >** ***name of device***

4 For each device not shared across the cluster, deactivate **Device is shared clusterwide**.

   Note By default, the **Device is shared clusterwide** setting is deactivated for devices detected as local and enabled for non-local devices. This setting allows storage host profiles to ignore local devices during compliance checks.

   The **Device is Shared Clusterwide** setting for PSA devices helps you determine which devices in the cluster should be configured by a host profile. Correctly setting this value for devices in the cluster eliminates compliance errors due to non-shared devices.

5 Remediate the host profile to the reference host for the changes to take effect.

Compliance failures with SAN Boot LUN Devices

This procedure resolves compliance failures for SAN boot LUN devices shared across the cluster, but logically local to the ESXihost.

To avoid this compliance failure from occurring, set the **Device is shared clusterwide** value to **False** before extracting the host profile from the reference host. You can deactivate the value by using the command `esxcli storage core device setconfig -d naa.xxxx --shared-clusterwide=false`, where *naa.xxxx* is the unique device identifier generated in naa format.

Prerequisites

Extract a host profile from a reference host. See How Do You Create a vSphere Host Profile? for instructions.

Procedure

1 Navigate to **Host Profiles** main view and select the host profile that you want to edit.

2 Click the **Configure** tab, and click **Edit Host Profile**.

3 Select **Storage configuration > Pluggable Storage Architecture configuration > PSA device sharing >** ***name of device***

4 Deactivate the **Device is shared clusterwide** in the host profile by deselecting the check box.

   When applying the host profile to the target host, the boot device settings for the remote boot LUN device are copied from the reference host into the target host.

5 (Optional) Select **Storage configuration > Pluggable Storage Architecture configuration > Host boot device configuration** and verify that the boot LUN ID is correctly captured.

6 Remediate the host profile to the reference host for the changes to take effect.

   If you must re-extract the host profile (for example, if you attach more shared SAN boot LUNs to your cluster), you do not need to reconfigure the **Device is Shared Clusterwide** setting for devices that you previously configured through ESXCLI.

Edit Settings for vSphere Host Profiles is Failing

Editing a vSphere host profile results in an error.

Problem

In a vCenter Server inventory upgraded to version 6.5, if you try to edit the settings for a host profile with version 5.1, one of the following errors might appear:

```
Unexpected status code: 503
```

or

```
There are no hosts available in the inventory at the version for the selected Host Profile
```

Cause

vSphere 6.5 supports only hosts and host profiles with version 5.5 and later.

Solution

- Extract a Host Profile from an already upgraded host to version 5.5. or later.

- Use the **Copy Settings from Host** option to copy the configuration settings from a host already upgraded to a version 5.5. or later.

  Note Using the **Copy Settings from Host** option overwrites the settings within the existing Host Profile or sets them to the default values.

vSphere Host Profile without an NFS Datastore

A host profile compliance check fails for NFS datastore.

Problem

When you confirm the compliance of your ESXi host to its attached Host Profile, a non-compliant status is present for the NFS datastore. The compliance check detects the mounted NFS datastore to the ESXi host as an additional datastore.

Cause

The remediate or compliance check failure occurs when the following two conditions take place:

- The extracted Host Profile does not have NFS storage (NasStorageProfile).
- The ESXi host, attached to the Host Profile, has an already mounted NFS storage.

Solution

1. Create a dummy NFS datastore in the Host Profile.
2. Deactivate the dummy NFS datastore so that the NFS storage profile is fully deactivated.

Upgraded Host is Not Compliant with a Legacy Host Profile

An upgraded ESXi host with attached legacy vSphere host profile results in a non-compliant status after reboot.

Problem

When you upgrade a host to the latest ESXi version and remediate the attached legacy host profile to that host, the compliance status might be updated to non-compliant after the host reboots.

Cause

You are using a legacy host profile, which is attached to an ESXi host version 6.7 or earlier and contains the following sub-profiles:

- `Misc.LogPort`
- `host/vim/vmvisor/plugins/vmware_*`

Solution

- Make the ESXi host compliant with the legacy host profile.
  a From the **Host Profiles** main view, right-click the host profile that you want to edit and select **Edit Host Profile**.
  b In the **Edit host profile** page, deactivate the sub-profile(s).
  c **Check Host Profile Compliance**.
- Upgrade the legacy host profile to the same version as the ESXi host.
  a Right-click the legacy host profile and select **Copy Settings from Host**.
  b Select the upgraded ESXi host from which you want to copy the configuration settings and click **OK**.